SOME CRYPTOGRAPHIC CHALLENGES

DAVE SILVERMAN

In his Kickshaws column (1969-1975) Dave Silverman frequently presented offbeat cryptograms for Word Ways readers to solve,

A Challenge

The Word Buff offers a pangrammatic cryptogram which is deceptively difficult to solve (both Darryl Francis and Ross Eckler failed to do so). Can Word Ways readers do it?

NS QSSZ QCF SLPRHS ZZF AECH XCBB XCBBRFSZ YECRQZO, CE XREYS KBCRZO

CA TBB XBRHJSCRO ARHSO; CRE BMDSO SISEGNPSES QSSZ QC WRTKDOTBISE FC

OPCN CQS PMO VROF KCQKSEQ CISE HCZSEQ OSBA-ZSOFERKF HSFPCZO:

RQKCQFECBBSZ JCCUS, ZERYO (XCF, OXSSZ), SFK.

For Cryptanalysts Only

The transmitting agency uses a different mode of encipherment for each of its receiver, and that's one heck of a weakness, for on the same day, at approximately the same time, your agents in Erewhon, Ecalpon, and Wohon, have intercepted three different cipher-texts, which you suspect (correctly) all overlie the same short plain-text message. Once you break through and read the message, you should be able to reconstruct the modes of encipherment. If we don't receive any solutions from you by the deadline for the August issue, we'll throw in a crib or two.

515-1 229-7 469-9: 122-4 510-2 591-2 328-42 41-17 17-4 173-10!

ADYTR MUDBR MOAYP UHDSE SUALM TQMXI MVAXX!

DEWRL TKEJY OTIST HIDEX EQLXV ZTUSH YZLBX!

Last time we challenged cryptanalysts with a short message, enciphered in three different ways, with the objective of reading the message and reconstructing all three modes of encipherment. Sean Reddick and Ross Eckler succeeded, and three other cryppies found everything but the last mode of encipherment. All breakthroughs presumably came by cracking the first, numerical code, consisting of 2- or 3-digit numbers followed by 1- or 2-digit numbers. Solvers deduced this was a book code with page number followed by word number on the indicated page. What book more simple than a dictionary and what dictionary more probable than the Merriam-Webster pocket version? It might be argued that even if the first cipher is recognized as a book code, the difficulty in determining what book was used is too great to make the challenge fair. However, once one assumes that the numbers represent dictionary entries, the determination of the dictionary is helpful but not absolutely necessary. The page numbers alone can generally be used to determine the message uniquely if the message is long enough, since the *relative* position of any given word

is approximately the same among virtually *all* dictionaries. In the case of shorter messages, a crib or a hint as to the message's meaning is probably necessary.

The second encipherment was by a reciprocal substitution cipher in which X was a fixed point, i.e. was enciphered by itself. Can you prove that this cipher must contain at least one other fixed point? The third cipher was the most difficult to reconstruct. It was a digraphic (two letters at a time) cipher known as a Playfair after its nineteenth-century inventor. The5-by-5 Playfair matrix is formed by taking any key phrase and writing it in, left to right, top to bottom neglecting repeated letters. The remaining cells are filled in in alphabetic order with the remaining letters. I and J traditionally occupy the cell to fit 26 letters into 25 cells. Having constructed the matrix, the encipherment of the message is done according to the following rules: (1) if the two plaintext letters are on different rows or columns, the cipher letters are the remaining two vertices of the rectangle in the order high-low, (2) if the plaintext letters occupy the same row (column), move one row right (one column down) to obtain the cipher letters, (3) if the two plaintext letters are the same, recast the message.

Reddick'sTriumph

Several years ago in the comic strip "Steve Roper" a reporter excitedly telephoned the following cipher message: 188-1-22 71-2-13 70-2-11 68-1-25 19-1-6 112-2-10 99-1-35! Sean Reddick immediately deduced that here was an underlying seven-word message and that a dictionary code ha been applied, each entry giving page, column and word-number. He was unable to find the dictionary then, and to this day has never found it. Nevertheless, he solved the crypt using the ratios involved and half a dozen dictionaries in order to get the probable range of each word as closely as possible. With a message that short, solution is bound to be nearly impossible, but Sean made a lucky guess, based on the fact that the reporter mentioned in what appeared to be a significant way that the plaintext message had been given to him by "the delivery boy". He documented his solution by sending it to a nationally-known columnist, who reported it a couple of weeks later when events in the comic strip bore out Sean's solution.

You have all the facts before you. Care to try to duplicate Sean Reddick's feat? My own effort (Wisconsin musical multimillionaire leads concert under pavilion) just does not pass muster.

Another Tricrypt

None of the three modes of encipherment could possibly be based on a unique plaintext message. And although Kickshaws believes that taken together they determine the message uniquely, we grant that they are not a very practical cryptographic device. Our main objective is to give the readers another chance at what we think will prove to be a not-so-outrageously difficult example as the one presented last issue. This time the encipherment modes are not hidden. The message, consisting of 17 words, can be read as a rhyming couplet. The first clue gives the meter, the second the word lengths, and the third gives the dictionary order of the words as they appear in the message. Have at it!

The first line consists of an iamb followed by four anapests; the second line consists of five iambs
Word lengths are 6 2 4 3 6 3 5 8 5 5 3 5 4 6 4 5 4
Dictionary order is 5 3 10 2 8 1 14 11 17 9 13 12 15 4 16 7 6

The time has come to settle accounts. In August 1972 we posed what turned out to be an outrageously difficulty cryptogram. In doing so we violated the professional puzzler's most important principle make it solvable. If we had experimented before printing the damned thing, we would have found that even the most seasoned, industrious expert couldn't crack it; there simply wasn't enough information there. By private correspondence with Bubonoctis [Mary Youngquist], the Word Botcher, and the Nova Caesarean [Ross Eckler], we found that the addition of *three* more clues was just barely enough to make it workable. We won't try any tricks like this again. We feel like a mystery writer who has kept all the clues to himself, and has thus violated the rules of his trade. We sentence ourselves to six weeks of working the inane Sunday crossword in the Los Angeles Herald-Examiner, in which the clue for GUY last Sunday was LOMBARDO.

The words have 3 1 1 1 2 1 1 2 1 1 1 2 1 2 1 2 1 syllables
The parts of speech are v prep n conj v pro pro n comp v art adj n v pro adj n
(where "comp" stands for a noun-verb compound)
The third word is a palindrome

Mad Avenue Strikes Again

Ordinarily, advertisers strive to make their message as clear as possible; in fact, most are designed to get through to the village idiot. The editor recently called to our attention an advertisement with a different twist. On the back of the magazine The American Statistician, Addison-Wesley led off an ad for three textbooks with the cryptic remark Y LUAEB H O DTYO AOOSGL. Care to try and figure out the hidden message? Although the slogan doesn't have the pizzazz of, say, "Let Esso put a tiger in your tank", it can equally well be applied to the sale of shoes, ships or sealing wax (or, for that matter, floor wax).